(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 February 2002 (28.02.2002)

PCT

(10) International Publication Number
WO 02/17114 A1

(51) International Patent Classification[7]: G06F 17/00, H04L 9/32

(21) International Application Number: PCT/AU01/01063

(22) International Filing Date: 27 August 2001 (27.08.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PQ 9692 25 August 2000 (25.08.2000) AU

(71) Applicant *(for all designated States except US)*: **THE TONEGUZZO GROUP PTY LIMITED** [AU/AU]; Level 9, 65 York Street, SYDNEY, New South Wales 2000 (AU).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **TONEGUZZO, Steve** [AU/AU]; Level 9, 65 York Street, SYDNEY, New South Wales 2000 (AU). **RIZVI, Aftab** [AU/AU]; Level 9, 65 York Street, SYDNEY, New South Wales 2000 (AU).

(74) Agent: **MAXWELL, Peter, Francis**; Level 6, 60 Pitt Street, Sydney, New South Wales 2000 (AU).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 02/17114 A1

(54) Title: BIOMETRIC AUTHENTICATION

(57) Abstract: Biometric information in encoded into digital signatures and digital certificates. Means are disclosed for issuing such signatures or certificates based upon confirmation of identity. Confirmation may be made by a referee in real time so that the digital signature or certificate is issued immediately. Confirmation may be made in a kiosk or vending machine environment, through a secure connection with a referee.

BIOMETRIC AUTHENTICATION

TECHNICAL FIELD

The present invention pertains to digital certificates and more particularly to a digital certificate that incorporates biometric data, as well as methods and apparatus for generating it.

BACKGROUND ART

A unique digital certificate assists in verifying the identity of a natural person as a sender of e-mail or other form of electronic correspondence or electronic transaction.

For digital certificates to become a mandatory and viable requirement for engaging in electronic transactions, there will need to be a method that better identifies the natural person uniquely.

Whilst the currently known Public Key Infrastructure (PKI) infrastructure, certificate and signature concepts are sound, the sub-optimal authentication of the owner of the certificate is a failing of current digital signatures.

DISCLOSURE OF THE INVENTION

The invention pertains to a verifiably unique certificate which combines a conventional digital certificate with data derived from bio-metric information and optionally (b) statistical data or bona fides (e.g. age, security classification, licence information, medical conditions).

The invention also provides management of the authentication processes.

MODES FOR CARRYING OUT THE INVENTION

A Public Key Infrastructure is a combination of hardware and software products, policies and procedures. A PKI is based on digital IDs known as digital certificates, which act like 'electronic passports'.

A typical PKI should consist of:

(a) A security policy for establishing top-level security, as well as the processes and principles for the use of cryptography. It is essentially the rules by which an administering organisation will handle keys and valuable information.

(b) Certificate Practice Statement (CPS). This is a document defining the operational procedures on how the security policy will be enforced and supported in practice, how certificates are issued, accepted and revoked, and how keys will be generated, registered and certified, where they will be stored, and how they will be made available to users.

(c) Certificate Authority (CA). The CA system is the trust basis of a PKI as it manages public key certificates for their whole life cycle. The CA issues certificates by binding the identity of a user or system to a public key with a digital signature. The CA establishes the schedule of expiry dates for certificates and ensures certificates are revoked when necessary by publishing Certificate Revocation Lists (CRLs). When implementing a PKI, an organisation can either operate its own CA system, or use the CA service of a Commercial CA or Trusted Third Party.

(d) Authentication Centre (AC) and Virtual Authentication Centre (VAC). An AC provides an optional intermediary between the user and the CA. It captures and authenticates the identity of the users and submits the certificate request to the CA. Whereas VAC provides an optional intermediary between the user and the CA, when the user submits the request for a certificate remotely with the means of facilities provided in the locations approved by the authentication centre (e.g.designated computing device, vending machines).

PKI-enabled Applications.

A PKI is a means to an end, providing the security framework by which PKI-enabled applications can be confidently deployed to achieve the end benefits, in this case the generation and use of a digital certificate which incorporates a unique biometric of its users.

The certificate is generated as follows: -

(a) The inputs may include: applicant's name, biometric data, address, country, date of birth, drivers licence number, social security number, passport number, tax-file number, birth certificate number and location of birth, public key of CA, official descriptor, expiry date, other data.

(b) The inputs are manipulated through an algorithm to produce a unique identification number.

(c) The CA identifier (assigned by the root CA) and the CA's URL is appended to the identification number to form a globally unique certificate.

(d) The certificate may incorporate a compliance seal. The compliance seal is a flag or image data, which the certificate carries in a readable field. The field may carry an image or cause a browser or plug-in to display an image. The image may be depicted within a browser window or as part of the browser. The compliance seal may be available (visual, mechanical, audible) on the browser or on the resource. Associated with the availability of the compliance seal is a link to the issuing CA (for example this link will take the user to the home page of the CA from which complaints may be lodged, the CPS may be available, etc).

In addition to generally accepted privacy and security guidelines (e.g. Guidelines issued by Defence Signals Directorate, Australia), special security arrangements should be made to secure the public/private key pair for CA,

resources (hardware and software) involved in the production and delivery of the biometric certificate. Strong encryption would be implied in delivering the biometric certificate from the CA to the user.

Certificate Practice Statement

Whole or part of this document (CPS) may, or may not be, publicly available.

The CPS document will consist of, but is not limited to, procedures for the following:

(a) PKI Infrastructure

(b) Organisational relationships

(c) Public policy and legislative matters.

(d) AC and CA standard operating internal controls and procedures.

(e) Privacy Policy.

(f) Security classifications.

(g) Codes of conduct.

(h) Fees and charges.

(i) List of acceptable *bona-fides* for all stakeholders.

(j) Application for certificate.

(k) Method of generating a unique certificate number.

(l) Generation and security of digital certificate

(m) Procedure for manual authentication and issue.

(n) Procedure for virtual authentication and issue.

(o) Procedure for use of a certificate.

(p) Requirements to be a referee.

(q) Auditing prior to application.

(r) Ongoing auditing.

(s) Terms and conditions.

(t) Rules of use.

(u) Delivery of digital certificate and seal.

(v) Revocation of digital certificate and seal.

(w) Distribution and usage of revocation and attribute tables.

(x) Frequently asked questions.

(y) User help

(z) Complaints mechanisms.

(aa) Metrics and statistical analysis.

(bb) Distribution, installation, operation and security of applications..

(cc) *General information.*

(dd) Enforcement mechanisms and penalties.

(ee) Any other applicable information.

(ff) Renewal in the event of an accident, plastic surgery or genetic therapy.

(gg) Maintenance of audit trails.

(hh) Eligibility criteria for witnesses and digital referees.

(ii) Criteria, guidelines and responsibility of the accredited organizations acting as a digital referees.

Accordingly, the invention provides a method of combining the existing digital certificate technology with any one or a combination of (a) data derived from bio-metric information and (b) statistical data (e.g. age, security classification, licence information, medical conditions).

The invention also provides management of the authentication processes.

The certificate of the present invention incorporates a signature derived from an algorithm which operates on biometric data, such as genetic input, blood type, facial data, finger or iris image data, voice data, etc. The certificate

also includes a uniquely allocated number or signature of the authenticating authority, a check digit or crc.

The certificate of the present invention may be securely stored in electronic, optical, magnetic, physical, biological or printed form.

Four methods of obtaining an authenticated biometric certificate are as follows: -

(a) Remotely with authentication supplied via "trusted" parties who have an established digital signature, i.e. "digital referee". The fact that a party is eligible to be a digital referee may be an attribute of their digital signature.

(b) Remotely with authentication supplied via the provision of acceptable data or facsimile of acceptable documents which is subject to verification through the data or document issuing authorities as referee.

(c) Remotely, by assessing documents presented by the applicant, and confirmed via trusted third parties.

(d) In person with authentication supplied via the provision of acceptable data or acceptable documents, which may be subject to verification through the data issuing authorities as referee.

These methods are explained in the following examples:

Example 1: A candidate person presents themselves in front of a live digital biometric sampling device at a location approved by the certification authority (e.g. vending machine) and establishes a secure link, such as a network connection, with digital referees accompanying that person into a virtual authentication centre (VAC). A digital referee is a person who is a current biometric certificate user and who can verify, in real time, the identity of an applicant based on live biometric (and perhaps other data) data or other

bona fides (such as documents, other digital certificates etc.) offered by the applicant during (in real time) the authentication process. The term "real time" is used here as including network lag and data transit time as means simply: as fast as the network technology will reasonably allow. The referees observe the image (or other data) of the person and optionally confirm the answers to a few questions asked of the person. The referee may also confirm live, the taking of a biometric by the candidate. A genetic sample may be taken, the proper sampling being confirmed by the referee analysed and transformed into digital data. A positive ID from the referee results in a certificate being issued immediately. The certificate is preferably created using an algorithm which operates on the same biometric data offered by the applicant and used by the referee for the verification. In this example, the attendance of a digital referee would either have to be pre-arranged or may be conducted in real time through the aid of a device. That device (e.g. phone or mobile computer) may transmit the digital referee's signature, it may capture a biometric image of the digital referee or it may ask certain questions of the referee based on the signature attributes or other data. Essentially there must be a mechanism to authenticate a digital referee in real-time if the attendance of the digital referee to the digital authentication centre has not been pre-arranged.

Example 2: A person presents themselves in front of a live digital biometric sampling device (e.g. digital or optical recording equipment) at a location approved by the certification authority (e.g. kiosk, vending machine etc.) and establishes a secure link with a virtual authentication centre. In the absence of referees, questions might be asked based on electronically available information (e.g. credit card statement, phone bill, etc). In the alternative, a representative of an organization that issues or has authorised access to photo IDs may act as the digital referee by comparing the live image

to networked stored resources, such as a company's stored image and optionally asking questions related to data within their or another database and providing only verification of identity or refusal to the VAC. Verification by the referee, in real time, results in the certificate being issued.

Example 3: A person presents themselves in front of a live digital biometric sampling device at a location approved by the certification authority (e.g. vending machine) and establishes a secure link with a virtual authentication centre. A static image of the applicant's face on a facsimile of a drivers licence or passport or other approved document (optionally scanned by the machine) is transmitted to the virtual interviewer at the virtual authentication centre. The passport and or driver's licence or other document details are verified by the virtual certification centre by comparing the applicant's transmitted document image with the live transmission of the applicant's image. If verified, both are then optionally compared to an image provided by the issuer of the document against the issuing authority's transmission of the same image of the supporting documents and a positive match results in the certificate being subsequently issued.

Example 4: A person presents themselves in the physical authentication centre (offices of the certificate issuing authority or its agents). Fills in the application form for the biometric digital certificate and submits it with the original driver's licence, the passport or other approved documents to the issuing officer. The applicant is presented in front of a live digital biometric sampling device and photograph or biometric data is taken. The passport and/or driver's licence or other documents are verified by the authentication centre against the issuing authority of the supporting documents and a certificate is issued on verification of these documents.

In use, the recipient of the user's certification may wish to verify that it was the user, and not an impostor, that sent the certificate. This requires that the recipient challenge the user to provide:

(a) Information uniquely known to the user;

Recipient initiates a new transaction between VAC and user. VAC pushes a browser window (or equivalent means of communication) to user. User answers VAC's questions. VAC verifies the answers and notifies the recipient whether the actual user is online or some one else is using the users certificate.

(b) Information gleaned from electronic records about the user;

By prior arrangement/consent to allow details of the electronic information such as phone bill or credit card details, etc. are conveyed to VAC for real time use between VAC and user. VAC may ask a few questions from the electronic information they have. If the user's response is correct, VAC sends the confirmation to the recipient that the user online is the actual user otherwise a negative response is sent to the recipient.

(c) Real time verification using networked equipment;

The applicant is verified in real time using the equipment, e.g., digital recorder, finger print or genetic sampling device, etc. attached to the applicants networked equipment on the request of the recipient or on random intervals.

It will be understood that a person's biometrics may change. When obtaining the certificate, a user may be compelled to agree to update their biometric containing certificate in the advent that a biometric altering event (BAE) occurs before the expiry of the certificate. A BAE may be genetic therapy, plastic surgery, disfiguring injury, etc. This also applies to the

alteration of any data field embodied in the certificate such as date of birth, name, address, etc.

Industrial Application: At the present time there is great concern amongst governments and industry over the ability to identify the country of origin and age of an individual wishing to partake in internet gambling. This patent, effectively implemented would provide a viable solution to exclusion of minors and not permitting residents of certain jurisdictions to play prohibited games by providing reliable and secure authentication of a user.

CLAIMS

1. A digital certificate, for use by a person, wherein:

the certificate incorporates data derived from an algorithm which operates on bio-metric information which identifies the person.

2. The digital certificate of claim 1, wherein:

the data is in the form of a digital signature derived from the algorithm which operates on biometric including any one of the group comprising: facial image data, genetic information, blood type information, finger or iris image.

3. A method of composing a digital certificate, comprising the steps of:

establishing a secure connection between a digital referee and a person;

using the referee to confirm a biometric presented to the referee in real time;

issuing the certificate if the referee can confirm the biometric.

4. The method of composing a digital certificate of claim 3, further comprising the step of:

using the referee to confirm a bona fide or other biometric presented to the referee in real time;

issuing the certificate if the referee can confirm the bona fide or other biometric.

5. The method of composing a digital certificate of either of claims 3 or 4, wherein:

the biometric or other biometric is operated on by the algorithm and thereby incorporated into the digital certificate.

6. The method of composing a digital certificate of either of claims 3 or 4, further comprising the step of:

authenticating the referee to the person in real time.

7. The method of composing a digital certificate of either of claims 3 or 4, wherein:

the method occurs in real time and results in a digital certificate that the person can access immediately.

8. The method of composing a digital certificate of either of claims 3 or 4, wherein:

the biometric or bona fide or other biometric is an approved document which is compared by the referee to a stored networked resource.

9. The method of composing a digital certificate of claim 8, wherein:

the stored network resource is obtained from an agency that issued the approved document.

10. The method of composing a digital certificate of either of claims 3 or 4, wherein:

the referee confirms the biometric or bona fide other biometric with reference to networked stored resources in real time.

11. The method of composing a digital certificate of claim 4, wherein::

biometric or bona fide or other biometric data is obtained from the person in real time and data about it is incorporated into the certificate.

12. The method of composing a digital certificate of either of claims 3 or 4, wherein:

the method is practiced utilising a vending machine or kiosk to submit the biometric or other biometric to the referee.

13. The method of composing a digital certificate of either of claims 3 or 4, wherein:

the biometric or bona fide or other biometric is an approved document which is transmitted to the referee and compared by the referee to a live transmission from the person.

14. The method of composing a digital certificate of claim 13, wherein:

the referee then confirms the biometric or bona fide or other biometric with reference to networked stored resources in real time.

15. The method of composing a digital certificate of either of claims 3 or 4, wherein:

the referee confirms a challenge question put to the person by the referee in real time.

16. The method of composing a digital certificate of claim 15, wherein:

the challenge question is either composed or conferred by reference to electronic resources accessible to the referee in real time.

17. A method of composing a digital signature, comprising the steps of:

obtaining a biometric of a person;

incorporating the biometric into a digital signature derived from an algorithm which operates on the biometric, the biometric comprising any one of the group of: facial image data, genetic information, blood type information, finger or iris image.

18. A method of composing a digital certificate, comprising the steps of:

obtaining a digital signature as claimed in claim 17; then

incorporating the signature into a digital certificate.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU01/01063

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. [7]: G06F 17/00, H04L 9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPAT USPTO (KEYWORDS): CERTIFICATE? BIOMETRIC, FINGERPRINT, IRIS, FACE, BLOOD, GENETIC, VERIF+, CONFIRM+, REFEREE, THIRD PARTY

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5712914 A (AUCSMITH et al) 27 January 1998 See whole document	1-2,17-18
X	WO 98/50875 A (GTE GOVERNMENT SYSTEMS CORPORATION) 12 November 1998 See whole document	1-2,17-18
X	EP 859488 A2 (ARCANVS) 19 August 1998 See whole document	1-2,17-18

☐ Further documents are listed in the continuation of Box C ☒ See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 November 2001	24 NOV 2001
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	Authorized officer **Stephen Lee** Telephone No : (02) 6283 2205

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/AU01/01063

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
US	5712914	WO	9908418	US	5878144	US	6175626
		AU	39750/97	EP	1002392		
WO	9850875	AU	74848/98	BR	9808737	EP	980559
		US	6105010	US	6202151	US	6208746
		US	6310966				
EP	859488	US	5872848	US	6085322		

END OF ANNEX